IN THE CLAIMS

This listing of the claim will replace all prior versions and listings of claim in the present application.

Listing of Claims

1. (currently amended)An information processing method for calculating x*(2^n) mod P for an input value x larger than a prime number P, the operator ^ denoting power, wherein:

the value x*(2^n) mod P is calculated without explicitly obtaining x mod P, by:

calculating or previously preparing 2^(2m+n) mod P when the input value x has to be transformed into x*(2^n) mod P, the number n denoting the number of bits necessary and sufficient for storing the modulus P and the number m denoting the number of bits necessary for storing the input value x;

calculating x1 = x*2^(2m+n)*(2^(-m)) mod P = x*2^(m+n) mod P by Montgomery modular multiplication; and

calculating x2 ~~:~~= x1*(2^(-m)) mod P = x*(2^n) mod P.

2. (currently amended)An information processing method for calculating x*(2^n) mod P for an input value x larger than a prime number P, the operator ^ denoting power, wherein:

the value x*(2^n) mod P is calculated without explicitly obtaining x mod P, by:

calculating or previously preparing 2^(m+2n) mod P when the input value x has to be transformed into x*(2^n) mod P, the number n denoting the number of bits necessary and sufficient for storing the modulus P and the

number m denoting the number of bits necessary for storing the input value x;

calculating x1 = x*2^(m+2n)*(2^(-m)) mod P = x*2^(2n) mod P by Montgomery modular multiplication; and

calculating x2 := x1*(2^(-n)) mod P = x*(2^n) mod P.

Claim 3 (canceled).

4. (new) The RSA cryptosystem method using Chinese Remainder Theorem comprising the steps of:

inputting an input value X;

calculating mod P using the information processing method according to claim 1 and encrypting the x; and

storing the encrypted x.

5. (new) The RSA cryptosystem method using Chinese Remainder Theorem comprising the steps of:

inputting an input value x;

calculating mod P using the information processing method according to claim 2 and encrypting the x; and

storing the encrypted x.

6. (new) An information processing apparatus for calculating x*(2^n) mod P for an input value x larger than a prime number P, the operator ^ denoting power,

wherein the number n denotes the number of bits necessary and

sufficient for storing the modulus P and the number m denotes the number of bits necessary for storing the input value x,

wherein the information processing apparatus comprises Montgomery modular multiplication and the Montgomery modular multiplication calculates

$$x1 = x*2^{(2m+n)}*(2^{(-m)}) \bmod P = x*2^{(m+n)} \bmod P$$

and calculates

$$x2 = x1*(2^{(-m)}) \bmod P = x*(2^n) \bmod P.$$